					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P09					Τίτλος εγγράφου: **Πολιτική Τηλεργασίας**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τις υποχρεωτικές απαιτήσεις για την ασφαλή εκτέλεση τηλεργασίας, συμπεριλαμβανομένης της χρήσης των πληροφοριακών συστημάτων του οργανισμού, της πρόσβασης σε δεδομένα και της εκτέλεσης εργασιακών καθηκόντων εκτός των εταιρικών εγκαταστάσεων.

1.2 Διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριακών περιουσιακών στοιχείων στα οποία παρέχεται απομακρυσμένη πρόσβαση και θεσπίζει ελέγχους για τον μετριασμό των κινδύνων που συνδέονται με κατανεμημένα περιβάλλοντα εργασίας.

1.3 Η πολιτική καλύπτει τις απαιτήσεις του ISO/IEC 27001:2022, Παράρτημα Α, Έλεγχος 6.7, μέσω της εφαρμογής τεχνικών και διαδικαστικών δικλίδων ασφαλείας προσαρμοσμένων στις συνθήκες τηλεργασίας.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλο το προσωπικό που έχει εξουσιοδοτηθεί να εργάζεται εξ αποστάσεως, συμπεριλαμβανομένων των εξής:

2.1.1 Εργαζόμενοι (πλήρους απασχόλησης, μερικής απασχόλησης, συμβασιούχοι)

2.1.2 Εξωτερικοί πάροχοι υπηρεσιών, σύμβουλοι, προμηθευτές και λοιποί τρίτοι

2.1.3 Προσωρινό προσωπικό και προσωπικό έργου, με εγκεκριμένη απομακρυσμένη πρόσβαση (VPN, διαχείριση φορητών συσκευών)

2.2 Καλύπτει:

2.2.1 Πρόσβαση σε πληροφοριακά συστήματα του οργανισμού μέσω VPN ή άλλων εγκεκριμένων εργαλείων απομακρυσμένης πρόσβασης

2.2.2 Χειρισμό ευαίσθητων και ρυθμιζόμενων δεδομένων εκτός ασφαλών εγκαταστάσεων

2.2.3 Χρήση εξοπλισμού ιδιοκτησίας του οργανισμού ή χρήση προσωπικών συσκευών (BYOD)

2.2.4 Φυσικές και λογικές δικλίδες ασφαλείας σε απομακρυσμένα περιβάλλοντα

2.3 Η πολιτική εφαρμόζεται σε όλες τις γεωγραφικές περιοχές και ζώνες ώρας όπου ο οργανισμός επιτρέπει την τηλεργασία, είτε σε τακτική βάση είτε έκτακτα είτε στο πλαίσιο συμβάντων επιχειρησιακής συνέχειας.

3. Στόχοι

3.1 Να διασφαλίζεται ότι μόνο εξουσιοδοτημένα άτομα μπορούν να αποκτούν απομακρυσμένη πρόσβαση σε εσωτερικά συστήματα και πληροφορίες.

3.2 Να επιβάλλεται η χρήση κρυπτογράφησης, πολυπαραγοντικού ελέγχου ταυτότητας και προστασίας τερματικών σημείων σε όλες τις διαδρομές απομακρυσμένης πρόσβασης.

3.3 Να διατηρείται κατάλληλο επίπεδο ασφάλειας έναντι απειλών όπως το ηλεκτρονικό ψάρεμα, το κακόβουλο λογισμικό, η μη εξουσιοδοτημένη εξαγωγή δεδομένων και η μη εξουσιοδοτημένη έκθεση συστημάτων.

3.4 Να ρυθμίζεται ο τρόπος με τον οποίο ευαίσθητα δεδομένα διαβιβάζονται, αποθηκεύονται ή εκτυπώνονται σε περιβάλλοντα εκτός εγκαταστάσεων.

3.5 Να ενσωματώνονται μέτρα φυσικής ασφάλειας που περιορίζουν την ορατότητα και τη μη εξουσιοδοτημένη παρατήρηση κατά τη διάρκεια απομακρυσμένων συνεδριών.

3.6 Να διασφαλίζεται η συμμόρφωση με διεθνείς κανονιστικές απαιτήσεις σχετικά με την απομακρυσμένη πρόσβαση σε δεδομένα, συμπεριλαμβανομένου του ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ και του Κανονισμού DORA της ΕΕ.

4. Ρόλοι και αρμοδιότητες

4.1 Ανώτατη Διοίκηση

4.1.1 Εγκρίνει την παρούσα πολιτική και διασφαλίζει ότι διατίθενται οι απαιτούμενοι πόροι και ότι αυτή ενσωματώνεται στις λειτουργίες Ανθρώπινου Δυναμικού, Πληροφορικής και ασφάλειας.

4.1.2 Εγκρίνει τα κριτήρια επιλεξιμότητας για τηλεργασία και την εφαρμογή τους στις επιχειρησιακές μονάδες.

4.2 Επικεφαλής Ασφάλειας Πληροφοριών / Υπεύθυνος ΣΔΑΠ

4.2.1 Είναι υπεύθυνος για την παρούσα πολιτική, τη συντηρεί και διασφαλίζει την ευθυγράμμισή της με τη διάθεση ανάληψης κινδύνου και τις κανονιστικές υποχρεώσεις.

4.2.2 Καθορίζει τους ελέγχους ασφάλειας για την απομακρυσμένη πρόσβαση (π.χ. κρυπτογράφηση, προστασία τερματικών σημείων, χρονικά όρια συνεδρίας).

4.2.3 Εγκρίνει τη διαχείριση εξαιρέσεων και παρακολουθεί την αποτελεσματικότητα των ελέγχων.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Απαιτήσεις ανασκόπησης και επικαιροποίησης

9.1 Συχνότητα ανασκόπησης

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται ετησίως ή συχνότερα όταν προκύπτει ένα από τα ακόλουθα:

9.1.1.1 Εισαγωγή νέων τεχνολογιών απομακρυσμένης πρόσβασης

9.1.1.2 Σημαντική επέκταση της τηλεργασίας (π.χ. πρωτοβουλίες υβριδικού μοντέλου εργασίας)

9.1.1.3 Εμφάνιση νέων απειλών, ευπαθειών ή περιστατικών που συνδέονται με απομακρυσμένα περιβάλλοντα

9.1.1.4 Αλλαγές στο σχετικό νομικό ή κανονιστικό πλαίσιο

9.2 Ιδιοκτησία και διαδικασία ανασκόπησης

9.2.1 Ιδιοκτήτης της πολιτικής είναι ο Επικεφαλής Ασφάλειας Πληροφοριών. Η ανασκόπηση πρέπει να συντονίζεται με:

9.2.1.1 Λειτουργίες και Αρχιτεκτονική Πληροφορικής

9.2.1.2 Ανθρώπινο Δυναμικό και Εγκαταστάσεις (για επιχειρησιακές και χωρικές επιπτώσεις)

9.2.1.3 Υπεύθυνο Προστασίας Δεδομένων (για την προστασία προσωπικών δεδομένων και τους ελέγχους διασυνοριακών δεδομένων)

9.2.2 Οι επικαιροποιήσεις της πολιτικής πρέπει:

9.2.2.1 Να εγκρίνονται από την Επιτροπή Καθοδήγησης ΣΔΑΠ

9.2.2.2 Να γνωστοποιούνται σε όλο το επηρεαζόμενο προσωπικό και τους αναδόχους

9.2.2.3 Να ενσωματώνονται στο υλικό ένταξης και στην επαναληπτική εκπαίδευση

9.3 Έλεγχος εγγράφου και διανομή

9.3.1 Η πολιτική πρέπει να περιλαμβάνει έλεγχο εκδόσεων, ημερομηνία έναρξης ισχύος και ιστορικό μεταβολών.

9.3.2 Οι καταργημένες εκδόσεις πρέπει να διατηρούνται σύμφωνα με την Πολιτική Διαχείρισης Εγγράφων (P14).

9.3.3 Οι αναθεωρημένες εκδόσεις πρέπει να ενεργοποιούν υποχρεωτική εκ νέου βεβαίωση αποδοχής για χρήστες που είναι επιλέξιμοι για τηλεργασία.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική λειτουργεί σε συνδυασμό με τις εξής:

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τη βασική γραμμή για τον ασφαλή χειρισμό περιουσιακών στοιχείων, η οποία εφαρμόζεται σε όλα τα περιβάλλοντα εργασίας, συμπεριλαμβανομένης της τηλεργασίας.

10.1.2 P3 – Πολιτική Αποδεκτής Χρήσης: Διέπει την ορθή χρήση συσκευών και συστημάτων του οργανισμού κατά τις συνεδρίες τηλεργασίας.

10.1.3 P4 – Πολιτική Ελέγχου Πρόσβασης: Διασφαλίζει ότι τα δικαιώματα απομακρυσμένης πρόσβασης ακολουθούν την αρχή του ελαχίστου προνομίου και κατάλληλους μηχανισμούς αυθεντικοποίησης.

10.1.4 P6 – Πολιτική Διαχείρισης Κινδύνων: Καθορίζει πώς οι κίνδυνοι τηλεργασίας αναγνωρίζονται, αντιμετωπίζονται και παρακολουθούνται στο πλαίσιο του ΣΔΑΠ.

10.1.5 P12 – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Απαιτεί απογραφή και διαχείριση διαμόρφωσης για όλες τις συσκευές που χρησιμοποιούνται απομακρυσμένα.

10.1.6 P22 – Πολιτική Καταγραφής και Παρακολούθησης: Διασφαλίζει ότι οι απομακρυσμένες συνεδρίες παρακολουθούνται, ελέγχονται και διατηρούνται σύμφωνα με τις υποχρεώσεις συμμόρφωσης.

10.1.7 P14 – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Καθορίζει κανόνες χειρισμού δεδομένων σχετικούς με την τηλεργασία, συμπεριλαμβανομένων των αφαιρούμενων μέσων και της διάθεσης συσκευών.

10.2 Οι πολιτικές αυτές διασφαλίζουν συλλογικά ότι η τηλεργασία είναι ασφαλής, συμμορφούμενη και εφαρμόζεται σε όλες τις λειτουργίες και γεωγραφικές περιοχές.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική ευθυγραμμίζεται με διεθνώς αναγνωρισμένα πλαίσια ασφάλειας, προστασίας δεδομένων και διαχείρισης κινδύνων ΤΠΕ, ώστε να διασφαλίζονται ασφαλείς, ιχνηλάσιμες και συμμορφούμενες πρακτικές τηλεργασίας.

11.2 ISO/IEC 27001

11.2.1 Ρήτρα 6.1.3 – Σχεδιασμός αντιμετώπισης κινδύνων: Η παρούσα πολιτική συμβάλλει στην αντιμετώπιση των κινδύνων που συνδέονται με την απομακρυσμένη πρόσβαση και τα κατανεμημένα περιβάλλοντα εργασίας.

11.2.2 Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί την εφαρμογή ελέγχων για συστήματα στα οποία παρέχεται πρόσβαση εκτός των εγκαταστάσεων του οργανισμού.

11.2.3 Παράρτημα Α, Έλεγχος 6.7 – Τηλεργασία: Η παρούσα πολιτική καλύπτει πλήρως τους απαιτούμενους ελέγχους για την ασφάλεια πληροφοριών όταν το προσωπικό εργάζεται εκτός των εγκαταστάσεων του οργανισμού, συμπεριλαμβανομένων φυσικών και λογικών δικλίδων ασφαλείας, διακυβέρνησης πρόσβασης και παρακολούθησης της συμπεριφοράς των χρηστών.

11.3 ISO/IEC 27002:2022 – Έλεγχος 6

11.3.1 Ο έλεγχος αυτός επιβάλλει διαδικαστικές και τεχνικές δικλίδες ασφαλείας για την τηλεργασία. Περιλαμβάνει απαιτήσεις για την ασφάλεια συσκευών, τις μεθόδους πρόσβασης, τις πρακτικές χειρισμού δεδομένων, τις περιβαλλοντικές δικλίδες ασφαλείας και τη διαχείριση εμπλεκόμενων τρίτων μερών, οι οποίες εφαρμόζονται μέσω της παρούσας πολιτικής.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Remote Access): Υποστηρίζεται άμεσα μέσω ελέγχων VPN, πολυπαραγοντικού ελέγχου ταυτότητας, καταγραφής συνεδριών και χορήγησης πρόσβασης βάσει ρόλων για απομακρυσμένους χρήστες.

11.4.2 AC-2 (Account Management): Ελέγχει την επιλεξιμότητα πρόσβασης, την ανάθεση απομακρυσμένων προνομίων και την απενεργοποίηση λογαριασμών.

11.4.3 SC-12 έως SC-13 (Cryptographic Protection, Cryptographic Key Establishment): Υλοποιούνται μέσω της υποχρεωτικής χρήσης VPN και πλήρους κρυπτογράφησης δίσκου για απομακρυσμένα τερματικά σημεία.

11.4.4 MP-5 (Media Transport Protection) και PE-18 (Location of Information System Components): Οι οδηγίες τηλεργασίας επιβάλλουν προστασία κατά τη μεταφορά και φυσικές δικλίδες ασφαλείας σε περιβάλλοντα εκτός εγκαταστάσεων.

11.4.5 AU-2, AU-6: Η καταγραφή και παρακολούθηση απομακρυσμένων συνεδριών υποστηρίζουν τις απαιτήσεις ελέγχου και απόκρισης σε περιστατικά.

11.5 ΓΚΠΔ της ΕΕ (2016/679)

11.5.1 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Η παρούσα πολιτική επιβάλλει ελέγχους ασφάλειας απομακρυσμένης πρόσβασης, κρυπτογράφησης και καταγραφής που είναι αναγκαίοι για την προστασία δεδομένων προσωπικού χαρακτήρα στα οποία παρέχεται απομακρυσμένη πρόσβαση ή που υποβάλλονται σε απομακρυσμένη επεξεργασία.

11.5.2 Άρθρο 5(1)(f): Διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα στα οποία παρέχεται πρόσβαση εκτός εγκαταστάσεων προστατεύονται από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια.

11.5.3 Αιτιολογική σκέψη 39: Τονίζει τον περιορισμό πρόσβασης, την ακεραιότητα και την εμπιστευτικότητα, ιδίως όταν οι συσκευές απομακρύνονται από ασφαλείς εγκαταστάσεις.

11.6 Οδηγία NIS2 της ΕΕ (2022/2555)

11.6.1 Άρθρο 21(2)(a, b, d): Απαιτεί η απομακρυσμένη πρόσβαση να προστατεύεται ως μέρος του πλαισίου διαχείρισης κινδύνων ΤΠΕ ενός οργανισμού. Η παρούσα πολιτική καλύπτει την απαίτηση για μέτρα ασφάλειας που περιλαμβάνουν έλεγχο πρόσβασης, ασφάλεια δεδομένων και οργανωτικές πολιτικές για απομακρυσμένα περιβάλλοντα.

11.6.2 Άρθρο 21(3): Ενισχύει την ευαισθητοποίηση σε θέματα ασφάλειας και την εφαρμογή της πολιτικής μεταξύ του προσωπικού που εργάζεται εκτός των κεντρικών εγκαταστάσεων.

11.7 Κανονισμός DORA της ΕΕ (2022/2554)

11.7.1 Άρθρο 5 – Πλαίσιο διακυβέρνησης και εσωτερικού ελέγχου: Η παρούσα πολιτική υποστηρίζει τις προσδοκίες ελέγχου κινδύνων ΤΠΕ για όλα τα επιχειρησιακά σενάρια, συμπεριλαμβανομένων των υβριδικών και απομακρυσμένων μοντέλων.

11.7.2 Άρθρο 8 – Πλαίσιο διαχείρισης κινδύνων ΤΠΕ: Οι κίνδυνοι απομακρυσμένης πρόσβασης αναγνωρίζονται, μετριάζονται και διέπονται μέσω τεχνικών και οργανωτικών μέτρων που εφαρμόζονται στην παρούσα πολιτική.

11.7.3 Άρθρο 9 – Ρυθμίσεις ανταλλαγής πληροφοριών: Προστατεύει από απομακρυσμένη διαρροή πληροφοριών που ανταλλάσσονται εντός δικτύων ψηφιακής επιχειρησιακής ανθεκτικότητας.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: Η παρούσα πολιτική υποστηρίζει την ασφαλή συνέχεια των επιχειρησιακών λειτουργιών ανεξαρτήτως φυσικής τοποθεσίας.

11.8.2 BAI06 – Managed IT Changes και BAI09 – Managed Assets: Διασφαλίζουν ότι οι συσκευές τηλεργασίας παρακολουθούνται, διαμορφώνονται με ασφαλή τρόπο και αντιμετωπίζονται ως κρίσιμα περιουσιακά στοιχεία.

11.8.3 APO13 – Managed Security: Προάγει ένα καθορισμένο πλαίσιο διακυβέρνησης ασφάλειας για απομακρυσμένα περιβάλλοντα.

11.8.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Καθιερώνει ότι η δραστηριότητα τηλεργασίας πρέπει να καταγράφεται, να ανασκοπείται και να ελέγχεται.